UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,796	12/24/2003	Leland A. Wallace	P3127-939	9789

21839 7590 06/25/2007
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
GERGISO, TECHANE	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
06/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/743,796	**Applicant(s)** WALLACE ET AL.
	Examiner Techane J. Gergiso T-G	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This is a non-Final Office Action in response to the communication filed one June 01, 2004.

2. Claims 1-48 have been examined and are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-12 and 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman (US Pat. No.: 5, 872, 917) in view of Yokota et al. (hereinafter referred to as Yokota, US Pat. No.: 7, 155, 607).

As per claim 1:

Hellman discloses a method for authenticating a computer, the method comprising the following steps:

issuing a credential from a first computer to a second computer (column 3: lines 30-45; figure 2A);

transmitting said credential and a computer challenge from the second computer to the first computer when the second computer is to be authenticated (figure 1: 16, 18; column 6: lines 23-45);

transmitting a response to said computer challenge from said first computer to said second computer (column 3: lines 30-45; column 6: lines 23-45); and

verifying said response with said second computer in order to authenticate (column 3: lines 1-45; column 5: lines 33-45).

Hellman does not explicitly disclose authentication of the computers. Yokota, in analogous art, however, discloses authentication of the first and the second computers (Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman to include authentication of the computers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide methods for authentication between apparatuses using a challenge and response system with improved security against spoofing, even when the same piece of challenge data that is used in a past authentication is reused as suggested by Yokota in (column 2: lines 22-27).

As per claim 2:

Hellman discloses a method, wherein the challenge is a random number generated by the second computer and the first computer computes the response to the challenge by performing a predetermined function on the random number (column 5: lines 56-67).

AS per claim 3:

Yokota discloses a method, wherein the second computer determines whether the first computer response is valid by performing the predetermined function on the random number and comparing the result to the response (column 5: lines 65-67; column 6: lines 1-15).

As per claim 4:

Hellman discloses a method, wherein the predetermined function is a hash function (column 7: lines 51-15).

As per claim 5:

Yokota discloses a method, wherein the second computer establishes a connection with the first computer when the response is valid (figure 7: S208).

As per claim 6:

Yokota discloses a method, wherein the first computer issues a credential with a time limit and the first computer determines whether the credential transmitted from the second computer is valid by determining the expiration time of the credential (column 3: lines 25035).

As per claim 7:

Hellman discloses a system for authenticating a computer, the system comprising:

a first computer (figure 1: 12); and

a second computer in communication with the first computer (figure 1: 14-22);

wherein the first computer and the second computer are configured to execute the following instructions (figure 1: 14-22):

issue a credential from the first computer to the second computer (column 3: lines 30-45; figure 2A);

transmit the credential and a challenge from the second computer to the first computer when the second computer is to be authenticated (figure 1: 16, 18; column 6: lines 23-45);

transmit a response to the challenge from the first computer to the second computer (column 3: lines 30-45; column 6: lines 23-45); and

verify the response with the second computer in order to authenticate (column 3: lines 1-45; column 5: lines 33-45).

Hellman does not explicitly disclose authentication of the computers. Yokota, in analogous art, however, discloses authentication of the first and the second computers (Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman to include authentication of the computers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide methods for authentication between apparatuses using a challenge and response system with improved security against spoofing, even when the same piece of challenge data that is used in a past authentication is reused as suggested by Yokota in (column 2: lines 22-27).

As per claim 8

Hellman discloses a method, wherein the second computer is configured to generate a challenge that is a random number and the first computer is configured to generate a response to the challenge by performing a predetermined function on the random number (column 7: lines 16-40).

As per claim 9:

Hellman discloses a method, wherein the second computer is configured to determine whether the response is valid by performing the predetermined function on the random number and comparing the result to the response (column 3: lines 60-67; column 5: lines 1-10).

As per claim 10:

Hellman discloses a method, wherein the predetermined function is a hash function (column 7: lines 51-15).

As per claim 11:

Yokota discloses a method, wherein the second computer establishes a connection with the first computer when the response is valid (figure 7: S208).

As per claim 12:

Yokota discloses a method, wherein the first computer issues a credential with a time limit and the first computer determines whether the credential transmitted from the second computer is valid by determining the expiration time of the credential (column 3: lines 25035).

As per claim 45:

Hellman discloses a system for authenticating a connection between computers, the system comprising:

first computing means (figure 1: 12); and

second computing means in communication with the first computing means (figure 1: 14-22);

wherein the first computing means is configured to issue a credential to the second computing means (figure 1: 14-22),

transmit and receive messages with the second computing means to verify the identity of the second computing means (column 3: lines 30-45; column 6: lines 23-45); and

the second computing means is configured to transmit the credential to the first computing means to authenticate therewith, and transmit and receive messages with the first computing means to verify the identity of the first computing means (column 3: lines 1-45; column 5: lines 33-45).

Hellman does not explicitly disclose authentication of the computers. Yokota, in analogous art, however, discloses authentication of the first and the second computers (Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman to include authentication of the computers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide methods for authentication between apparatuses using a challenge and response system with improved security against spoofing, even when the same piece of challenge data that is used in a past authentication is reused as suggested by Yokota in (column 2: lines 22-27).

As per claim 46:

Hellman discloses a system wherein the first computing means is a server computer and the second computing means is a client computer (figure 1: 10).

As per claim 47:

Hellman discloses a system wherein the server computer and the client computer are configured to:

issue a credential from the server computer to a client computer (column 3: lines 30-45; figure 2A);

generate a client challenge with the client computer (column 6: lines 57-67);

transmit the credential and the client challenge from the client computer to the server computer (figure 1: 16, 18; column 6: lines 23-45);

determine with the server computer whether the credential is valid (column 5: lines 50-60);

compute a server response to the client challenge and a server challenge with the server computer (column 6: lines 57-67);

transmit the server response and the server challenge from the server computer to the client computer (column 3: lines 30-45; column 6: lines 23-45);

determine with the client computer whether the server response is valid (column 5: lines 50-60);

compute a client response to the server challenge with the client computer (column 6: lines 57-67);

transmit the client response from the client computer to the server computer (column 3: lines 30-45; column 6: lines 23-45); and

determine with the server computer whether the client response is valid to verify and authenticate the computers (column 3: lines 1-45; column 5: lines 33-45).

5. Claims 13-44 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman (US Pat. No.: 5, 872, 917) in view of Yokota et al. (hereinafter referred to as Yokota, US Pat. No.: 7, 155, 607), and further in view of Kumar et al. (hereinafter referred to as Kumar, US Pat. No.: 6,535,980).

As per claim 13:

Hellman discloses a method for authenticating a computer, the method comprising the steps:

issuing a credential from a first computer to a second computer (column 3: lines 30-45; figure 2A);

generating with the second computer a first challenge (column 6: lines 57-67);

transmitting the credential and the first challenge from the second computer to the first computer (figure 1: 16, 18; column 6: lines 23-45);

determining with the first computer whether the credential is valid (column 5: lines 50-60);

computing a first response to the first challenge and generating a second challenge with the first computer (column 6: lines 57-67);

transmitting the first response and the second challenge from the first computer to the second computer (column 3: lines 30-45; column 6: lines 23-45);

determining with the second computer whether the second response is valid (column 5: lines 50-60);

computing a second response to the second challenge with the second computer (column 6: lines 57-67);

transmitting the second response from the second computer to the first computer (column 3: lines 30-45; column 6: lines 23-45); and

determining with the first computer whether the second response is valid to verify (column 3: lines 1-45; column 5: lines 33-45).

Hellman does not explicitly disclose authentication of the computers. Yokota, in analogous art, however, discloses authentication of the first and the second computers (Column

2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman to include authentication of the computers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide methods for authentication between apparatuses using a challenge and response system with improved security against spoofing, even when the same piece of challenge data that is used in a past authentication is reused as suggested by Yokota in (column 2: lines 22-27).

Hellman and Yokota do not explicitly disclose the first challenge, the first response, the second challenge, and the second response. Kumar, in analogous art, however, discloses the first challenge, the first response, the second challenge, and the second response (figure 1: 1, 2, Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman and Yokota to include the first challenge, the first response, the second challenge, and the second response. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a secure method of data transfer using a challenge response in which a correct response to a challenge is used to transmit the value "1", while a deliberately false response is made to transmit the value "0" as suggested by Kumar in (column 2: lines 22-27).

As per claim 24:

Hellman discloses a method computer-readable medium containing a program with instructions that execute the following procedure:

issue a credential from a first computer to a second computer (column 3: lines 30-45; figure 2A);

generate a first challenge with the second computer (column 6: lines 57-67);

transmit the credential and the first challenge from the second computer to the first computer (figure 1: 16, 18; column 6: lines 23-45);

determine with the first computer whether the credential is valid (column 5: lines 50-60);

compute a first response to the first challenge and generate a second challenge with the first computer (column 6: lines 57-67);

transmit the first response and the second challenge from the first computer to the second computer (column 3: lines 30-45; column 6: lines 23-45);

determine with the second computer whether the first response is valid to verify the first computer (column 5: lines 50-60);

compute a second response to the second challenge with the second computer; transmit the second response from the second computer to the first computer (column 6: lines 57-67); and

determine with the first computer whether the second response is valid to verify and authenticate the computers (column 3: lines 1-45; column 5: lines 33-45).

Hellman does not explicitly disclose authentication of the computers. Yokota, in analogous art, however, discloses authentication of the first and the second computers (Column

2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman to include authentication of the computers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide methods for authentication between apparatuses using a challenge and response system with improved security against spoofing, even when the same piece of challenge data that is used in a past authentication is reused as suggested by Yokota in (column 2: lines 22-27).

Hellman and Yokota do not explicitly disclose the first challenge, the first response, the second challenge, and the second response. Kumar, in analogous art, however, discloses the first challenge, the first response, the second challenge, and the second response (figure 1: 1, 2, Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman and Yokota to include the first challenge, the first response, the second challenge, and the second response. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a secure method of data transfer using a challenge response in which a correct response to a challenge is used to transmit the value "1", while a deliberately false response is made to transmit the value "0" as suggested by Kumar in (column 2: lines 22-27).

As per claim 35:

Hellman discloses a method and system for authenticating a computer, the system comprising:

a first computer (figure 1: 12); and

a second computer in communication with the first computer (figure 1: 14-22);

wherein the first computer and the second computer are configured to execute the following instructions (figure 1: 14-22):

issue a credential from the first computer to the second computer (column 3: lines 30-45; figure 2A);

generate a first challenge with the second computer (column 6: lines 57-67);

transmit the credential and the first challenge from the second computer to the first computer (figure 1: 16, 18; column 6: lines 23-45);

determine with the first computer whether the credential is valid (column 5: lines 50-60);

compute a first response to the first challenge and generate a second challenge with the first computer (column 6: lines 57-67);

transmit the first response and the second challenge from the first computer to the second computer (column 3: lines 30-45; column 6: lines 23-45);

determine with the second computer whether the first response is valid (column 5: lines 50-60);

compute a second response to the first challenge with the second computer (column 6: lines 57-67);

transmit the second response from the second computer to the first computer (column 3: lines 30-45; column 6: lines 23-45); and determine with the first computer whether the second response is valid to authenticate and verify the computers (column 3: lines 1-45; column 5: lines 33-45).

Hellman does not explicitly disclose authentication of the computers. Yokota, in analogous art, however, discloses authentication of the first and the second computers (Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman to include authentication of the computers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide methods for authentication between apparatuses using a challenge and response system with improved security against spoofing, even when the same piece of challenge data that is used in a past authentication is reused as suggested by Yokota in (column 2: lines 22-27).

Hellman and Yokota do not explicitly disclose the first challenge, the first response, the second challenge, and the second response. Kumar, in analogous art, however, discloses the first challenge, the first response, the second challenge, and the second response (figure 1: 1, 2, Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman and Yokota to include the first challenge, the first response, the second challenge, and the second response. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a secure method of data transfer using a challenge response in which a correct response to a challenge is used to transmit the value "1", while a deliberately false response is made to transmit the value "0" as suggested by Kumar in (column 2: lines 22-27).

As per claims 14, 25 and 36:

Hellman discloses a method, system and computer readable medium having instructions, wherein the second computer encrypts the credential before transmitting the credential to the first computer (column 2: lines 35-55).

As per claims 15, 26 and 37:

Hellman discloses a method, system and computer readable medium having instructions, wherein the first computer challenge is a random number generated by the second computer and the first computer computes a first response to the first challenge by performing a predetermined function on the random number (column 5: lines 56-67).

As per claims 16, 27 and 38:

Yokota discloses a method, system and computer readable medium having instructions, wherein the second computer determines whether the first response is valid by performing the predetermined function on the random number and comparing the result to the first response (column 5: lines 65-67; column 6: lines 1-15).

As per claims 17, 28 and 39:

Hellman discloses a method, system and computer readable medium having instructions, wherein the predetermined function is a hash function (column 7: lines 51-15).

As per claims 18, 29 and 40:

Hellman discloses a method, system and computer readable medium having instructions, wherein the second challenge is a random number generated by the first computer and the second computer computes a second response to the second challenge by performing a predetermined function on the random number (column 5: lines 56-67).

As per claims 19, 30 and 41:

Yokota discloses a method, system and computer readable medium having instructions, wherein the first computer determines whether the second response is valid by performing the predetermined function on the random number and comparing the result to the second response (column 5: lines 65-67; column 6: lines 1-15).

As per claims 20, 31 and 42:

Hellman discloses a method, system and computer readable medium having instructions, wherein the predetermined function is a hash function (column 7: lines 51-15).

As per claims 21, 32 and 43:

Yokota discloses a method, system and computer readable medium having instructions, wherein the first computer issues the credential with an expiration time and the first computer determines whether the credential transmitted from the second computer is valid by determining the expiration time of the credential (column 3: lines 25035).

As per claims 22, 33 and 44:

Yokota discloses a method, system and computer readable medium having instructions, wherein comprising the steps of:

encrypting the first challenge with the second computer before transmitting to the first computer (figure 14: 94);

decrypting the first challenge with the first computer before determining whether the first response is computed (figure 14: 103);

encrypting the first response and the second challenge with the first computer before transmitting (figure 14: 94);

decrypting the first response and the second challenge with the second computer before determining whether the first response is valid and the second response is computed (figure 14: 103);

encrypting the second response with the second computer before transmitting (figure 14: 94); and

decrypting the second response with the first computer before determining whether the second response is valid (figure 14: 103).

As per claims 23 and 34:

Yokota discloses a method and computer readable medium having instructions, wherein the credential is encrypted before issuing the credential to the second computer and the credential is decrypted by the first computer when returned by the second computer (figure 14: 103; figure 14: 94).

As per claim 48:

Hellman discloses a method of authentication performed between a first user and a second user with a computer, the method comprising the steps of:

issuing a credential from the first user to the second user (column 3: lines 30-45; figure 2A);

generating a first challenge with the second user (column 6: lines 57-67);

transmitting the credential and the first challenge to the first user (figure 1: 16, 18; column 6: lines 23-45);

determining with the first user whether the credential is valid (column 5: lines 50-60);

generating with the first user a first response to the first challenge and a second challenge (column 6: lines 57-67);

transmitting the first response and the second challenge to the second user (figure 1: 16, 18; column 6: lines 23-45);

determining with the second user whether the first response is valid (column 5: lines 50-60);

generating with the second user a second response to the second challenge (column 6: lines 57-67);

transmitting the second response to the first user (figure 1: 16, 18; column 6: lines 23-45); and

determining with the first user whether the second response is valid in order to authenticate and verify the first and second users (column 5: lines 50-60);

Hellman does not explicitly disclose authentication of the computers. Yokota, in analogous art, however, discloses authentication of the first and the second computers (Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman to include authentication of the computers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide methods for authentication between apparatuses using a challenge and response system with improved security against spoofing, even when the same piece of challenge data that is used in a past authentication is reused as suggested by Yokota in (column 2: lines 22-27).

Hellman and Yokota do not explicitly disclose the first challenge, the first response, the second challenge, and the second response. Kumar, in analogous art, however, discloses the first challenge, the first response, the second challenge, and the second response (figure 1: 1, 2, Column 2: lines column 2: lines 30-50). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hellman and Yokota to include the first challenge, the first response, the second challenge, and the second response. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a secure method of data transfer using a challenge response in which a correct response to a challenge is used to transmit the value "1", while a deliberately false response is made to transmit the value "0" as suggested by Kumar in (column 2: lines 22-27).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art.

Contact Information

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T-G
Techane Gergiso
Patent Examiner
Art Unit 2137

June 20, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER